UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/590,794	09/18/2006	Marc Girault	P1924US	2203

8968 7590 10/24/2008

DRINKER BIDDLE & REATH LLP
ATTN: PATENT DOCKET DEPT.
191 N. WACKER DRIVE, SUITE 3700
CHICAGO, IL 60606

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
10/24/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/590,794	GIRAULT ET AL.	
	Examiner	Art Unit	
	MICHAEL R. VAUGHAN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 September 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☒ Claim(s) *5 and 19* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on *25 August 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☒ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *8/25/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

The instant application having Application No. 10/590794 filed on 9/18/06 is presented for examination by the examiner.

Priority

Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). The certified copy has been received.

Claim Objections

Claims 5 and 19 are objected to because of the following informalities: the reference to (s, c) lacks antecedent basis.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:
Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-14, and 16 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The language of claim 1 is directed to a method of manipulating numbers which is an abstract idea. There is no concrete, tangible result defined in claim 1. A value is arrived at by performing some mathematics

to numbers. The claim should further define what the value can be used for, i.e. what purpose does it serve? It should be clear what the purpose the method has and not an abstraction of mathematics.

The dependent claims 2-14 and 16 are likewise rejected under 35 U.S.C. 101 because they fail to remedy the lack of statutory subject matter of claim 1.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:
The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-23 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The claims are generally narrative and indefinite, failing to conform to current U.S. practice. They appear to be a literal translation into English from a foreign document and are replete with grammatical and idiomatic errors. Examiner advises Applicant to carefully craft the claim language so that it is precise and clearly sets forth the metes and bounds of the claim. Phrases such as “mean of" creates a problem for ascertaining what is scoped by the claim.

As per claims 5, 8, 9, 13, 14, 19, 21, and 22, there is a question of whether “*s*” is the first or second factor and similarly “*c*” in claims 5 and 19. And then throughout the dependent claims to 5 and 19, the definition of ion of “s” and “y” change from being called a factor, and number, and secret key, and part of a secret key. The language

used to reference the factors and secret key needs to remain clear and concise throughout the claims. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-23 are rejected under 35 U.S.C. 102(e) as being anticipated by USP Application Publication 2006/0072743 to Naslund et al., hereinafter Naslund.

As per claim 1, Naslund teaches a method for performing a cryptographic operation in a device under the control of a security application, in which a cryptographic value (y) is produced in the device, by a calculation comprising at least one multiplication between two factors including a part at least of a secret key (s) associated with the device (0275),

wherein the first of the two factors of the multiplication has a determined number of bits L in binary representation, the second of the two factors of the multiplication is

constrained so that it comprises, in binary representation, several bits set to 1 with, between each pair of consecutive bits set to 1, a sequence of at least L - 1 bits set to 0, and the multiplication is achieved by assembling binary versions of the first factor, respectively shifted in accordance with the positions of the bits set to 1 of the second factor (0276).

As per claim 2, Naslund teaches the secret key (s) forms part of an asymmetric cryptographic key pair associated with the device (0274).

As per claim 3, Naslund teaches the device comprises a chip including hard-wired logic for producing the cryptographic value (0063).

As per claim 4, Naslund teaches the calculation of the cryptographic value furthermore comprises an addition or a subtraction between a pseudo-random number and the result of the multiplication (0275 and 0306).

As per claim 5, Naslund teaches the first and second factors and the pseudo-random number are dimensioned so that the pseudo-random number is greater than the result of the multiplication (0312).

As per claim 6, Naslund teaches the number of bits set to 1 of the second factor is chosen at most equal to the largest integer less than or equal to s1/L, where s1 is a predefined threshold less than the number of bits of the pseudo-random number (r) in binary representation (0168).

As per claim 7, Naslund teaches the two factors of the multiplication include, as well as said part of the secret key, a number provided to the device by the security application executed outside the device (0274).

As per claim 8, Naslund teaches the two factors of the multiplication include, as well as said secret key, a number provided by the device (0274).

As per claim 9, Naslund teaches part of the secret key (s) is said first factor of the multiplication (0275).

As per claim 10, Naslund teaches binary versions are disposed in respective intervals of like size in bits, said size corresponding to the total size of a usable space, divided by the number of bits set to 1 of the second factor of the multiplication, each binary version being placed in its respective interval as a function of a shift in accordance with the positions of the bits set to 1 of the second factor (0168).

As per claim 11, Naslund teaches part of the secret key (s) is the second factor of the multiplication (0276).

As per claim 12, Naslund teaches the secret key is stored in a memory support of the device by coding the positions of its bits set to 1 (0276).

As per claim 13, Naslund teaches the secret key (s) is stored in a memory support (-1-6) of the device by coding numbers of bits separating respectively lower bounds of intervals of (S- 1)/(n- 1) bits and lower bounds of blocks of bits allotted to the first factor (c) of the multiplication and each disposed in the associated intervals, S being the number of bits of the secret key and n the number of bits set to 1 of the secret key (0168 and 0276).

As per claim 14, Naslund teaches the secret key is stored in a memory support of the device by coding numbers of bits, each representative of the number of bits

separating two blocks of successive bits allotted to the first factor of the multiplication (0276).

As per claim 15, Naslund teaches the cryptographic value is produced so as to authenticate the device in a transaction with the security application executed outside the device (0304).

As per claim 16, Naslund teaches the cryptographic value is produced in the guise of electronic signature (0014).

As per claim 17, Naslund teaches a device with cryptographic function, comprising means of interfacing with a security application and means of calculation for producing a cryptographic value, the means of calculation comprising means of multiplication between two factors including a part at least of a secret key associated with the device (0275),

wherein a first of the two factors of the multiplication having a determined number of bits L in binary representation, and the second of the two factors of the multiplication being constrained so that it comprises, in binary representation, several bits set to 1 with, between each pair of consecutive bits set to 1, a sequence of at least L - 1 bits set to 0, the multiplication means comprise means for assembling binary versions of the first factor, respectively shifted in accordance with the positions of the bits set to 1 of the second factor (0276).

As per claim 18, Naslund teaches generating a pseudo-random number (r), the means of calculation comprising means for adding the result of the multiplication to or subtracting it from said pseudo- random number (0275 and 0306).

As per claim 19, Naslund teaches the first and second factors and the pseudo-random number are dimensioned so that the pseudo-random number is greater than the result of the multiplication (0312).

As per claim 20, Naslund teaches the means of calculation are embodied as hard-wired logic (0063).

As per claim 21, Naslund teaches part of the secret key is the first factor of the multiplication (0275).

As per claim 22, Naslund teaches part of the secret key (s) is the second factor of the multiplication (0276).

As per claim 23, Naslund teaches a memory adapted for storing data for coding the positions of the bits set to 1 of the secret key (0276).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure in included on the enclosed PTO-892 form.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./
Examiner, Art Unit 2431
/Syed Zia/
Primary Examiner, Art Unit 2431